(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 May 2000 (25.05.2000)

PCT

(10) International Publication Number
WO 00/30285 A1

(51) International Patent Classification[6]: H04K 1/00

(21) International Application Number: PCT/US99/27621

(22) International Filing Date:
19 November 1999 (19.11.1999)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/196,430 19 November 1998 (19.11.1998) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 08/996,758 (CIP)
Filed on 23 December 1997 (23.12.1997)

(71) Applicant *(for all designated States except US)*: ARCOT SYSTEMS, INC. [US/US]; 3200 Patrick Henry Drive, Suite 200, Santa Clara, CA 95054 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: KAUSIK, Balas, Natarajan [US/US]; 18079 Reed Knoll Road, Los Gatos, CA 95030 (US). VARADARAJAN, Rammohan [IN/US]; 11674 Seven Springs Drive, Cupertino, CA 95014 (US).

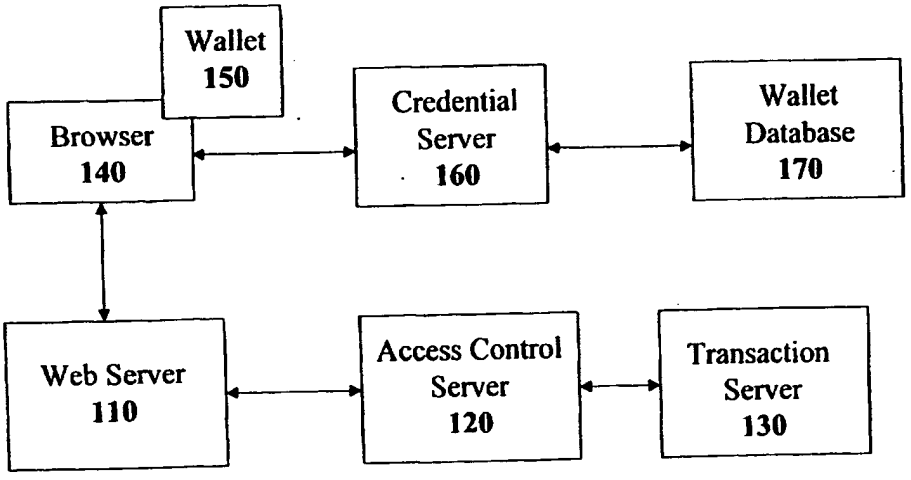
(74) Agents: LAURIE, Ronald, S. et al.; Skadden, Arps, Slate, Meagher & Flom LLP, 525 University Avenue, Palo Alto, CA 94301-1916 (US).

(81) Designated States *(national)*: AE, AU, BR, CA, CN, IL, IN, JP, KR, MX, NO, NZ, PL, RU, SG, US.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURE DISTRIBUTION OF AUTHENTICATION CREDENTIALS TO ROAMING USERS



(57) Abstract: A roaming user (150) needing an authentication credential (e.g., private key) (230) to access a computer server (110) to perform an electronic transaction may obtain the authentication credential (230) in an on-demand fashion from a credential server (160) accessible to the user over a computer network. In this way, the user is free to roam on the network without having to physically carry his authentication credential (230). Access to the credential (230) may be protected by one or more challenge-response protocols involving simple shared secrets, shared secrets with one-to-one hashing (210), or biometric methods such as fingerprint recognition. If camouflaging is used to protect the authentication credential (230), decamouflaging may be performed either at the credential server (140) or at the user's computer (160).

WO 00/30285 A1

Published:
— *with international search report*

(48) Date of publication of this corrected version:
19 July 2001

(15) Information about Corrections:
see PCT Gazette No. 29/2001 of 19 July 2001, Section II
Previous Correction:
see PCT Gazette No. 10/2001 of 8 March 2001, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 May 2000 (25.05.2000)

PCT

(10) International Publication Number
WO 00/30285 A1

(51) International Patent Classification[6]: H04K 1/00

(21) International Application Number: PCT/US99/27621

(22) International Filing Date:
19 November 1999 (19.11.1999)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/196,430 19 November 1998 (19.11.1998) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 08/996,758 (CIP)
Filed on 23 December 1997 (23.12.1997)

(71) Applicant *(for all designated States except US)*: ARCOT SYSTEMS, INC. [US/US]; 811 Hansen Way, Palo Alto, CA 94304-1023 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: KAUSIK, Balas, Natarajan [US/US]; 18079 Reed Knoll Road, Los Gatos, CA 95030 (US). VARADARAJAN, Rammohan [—/US]; 11674 Seven Springs Drive, Cupertino, CA 95014 (US).

(74) Agents: LAURIE, Ronald, S. et al.; Skadden, Arps, Slate, Meagher & Flom LLP, 525 University Avenue, Palo Alto, CA 94301-1916 (US).

(81) Designated States *(national)*: AU, CA, JP, NO, US.

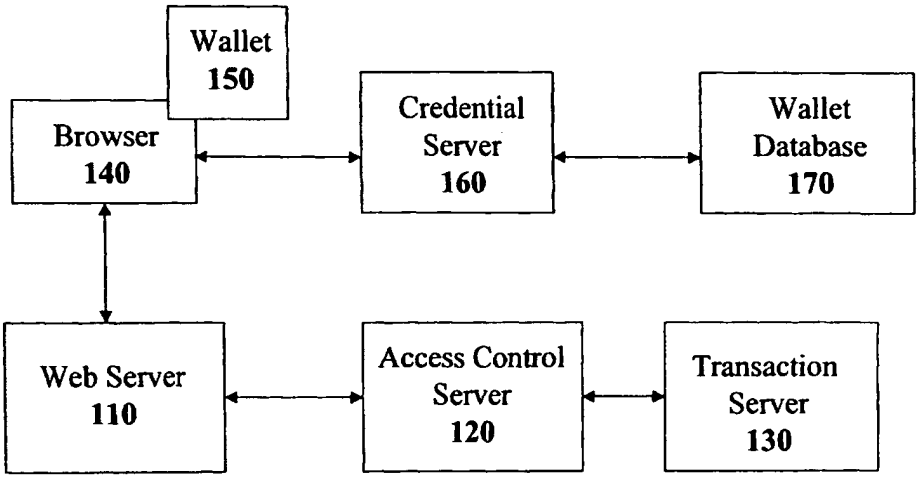
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

(48) Date of publication of this corrected version:
8 March 2001

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURE DISTRIBUTION OF AUTHENTICATION CREDENTIALS TO ROAMING USERS



(57) Abstract: A roaming user (150) needing an authentication credential (e.g., private key) (230) to access a computer server (110) to perform an electronic transaction may obtain the authentication credential (230) in an on-demand fashion from a credential server (160) accessible to the user over a computer network. In this way, the user is free to roam on the network without having to physically carry his authentication credential (230). Access to the credential (230) may be protected by one or more challenge-response protocols involving simple shared secrets, shared secrets with one-to-one hashing (210), or biometric methods such as fingerprint recognition. If camouflaging is used to protect the authentication credential (230), decamouflaging may be performed either at the credential server (140) or at the user's computer (160).

WO 00/30285 A1

(15) **Information about Correction:**
see PCT Gazette No. 10/2001 of 8 March 2001, Section II

For two-letter codes and other abbreviations. refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 May 2000 (25.05.2000)

PCT

(10) International Publication Number
WO 00/30285 A1

(51) International Patent Classification[6]: H04K 1/00

(21) International Application Number: PCT/US99/27621

(22) International Filing Date:
19 November 1999 (19.11.1999)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/196,430 19 November 1998 (19.11.1998) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 08/996,758 (CIP)
Filed on 23 December 1997 (23.12.1997)

(71) Applicant *(for all designated States except US)*: ARCOT SYSTEMS, INC. [US/US]; 3200 Patrick Henry Drive, Suite 200, Santa Clara, CA 95054 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: KAUSIK, Balas, Natarajan [US/US]; 18079 Reed Knoll Road, Los Gatos, CA 95030 (US). VARADARAJAN, Rammohan [IN/US]; 11674 Seven Springs Drive, Cupertino, CA 95014 (US).

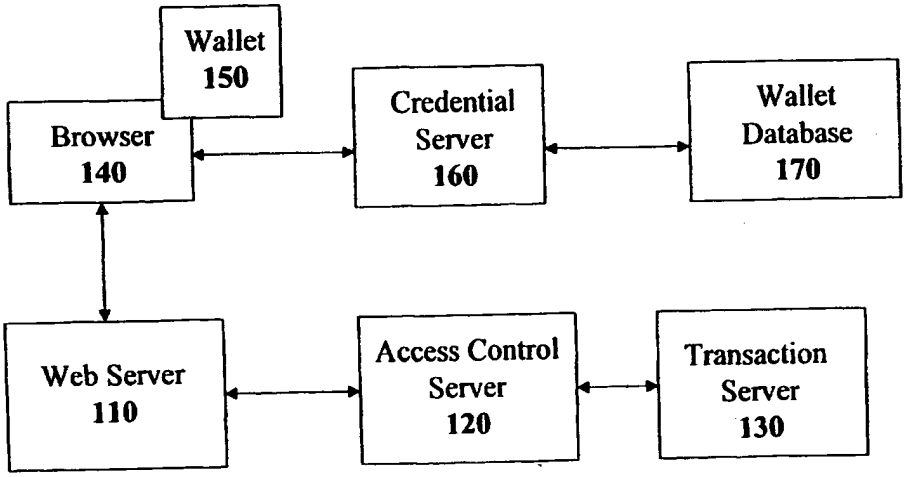
(74) Agents: LAURIE, Ronald, S. et al.; Skadden, Arps, Slate, Meagher & Flom LLP, 525 University Avenue, Palo Alto, CA 94301-1916 (US).

(81) Designated States *(national)*: AE, AU, BR, CA, CN, IL, IN, JP, KR, MX, NO, NZ, PL, RU, SG, US.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURE DISTRIBUTION OF AUTHENTICATION CREDENTIALS TO ROAMING USERS



(57) Abstract: A roaming user (150) needing an authentication credential (e.g., private key) (230) to access a computer server (110) to perform an electronic transaction may obtain the authentication credential (230) in an on-demand fashion from a credential server (160) accessible to the user over a computer network. In this way, the user is free to roam on the network without having to physically carry his authentication credential (230). Access to the credential (230) may be protected by one or more challenge-response protocols involving simple shared secrets, shared secrets with one-to-one hashing (210), or biometric methods such as fingerprint recognition. If camouflaging is used to protect the authentication credential (230), decamouflaging may be performed either at the credential server (140) or at the user's computer (160).

WO 00/30285 A1

Published:
— *with international search report*

(48) Date of publication of this corrected version:
19 July 2001

(15) Information about Corrections:
see PCT Gazette No. 29/2001 of 19 July 2001, Section II
Previous Correction:
see PCT Gazette No. 10/2001 of 8 March 2001, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.